Security Threats in Cloud-based Services

Panel #3

Moderator: Prof. Dr. Andreas Aßmuth

ComputationWorld 2023 & DataSys 2023

Nice, Saint-Laurent-du-Var, France

27th June 2023

Security Threats in Cloud-based Services Panel #3

Image: Image by Gerd Altmann from Pixabay

Statement: AGCS, "Allianz Risk Barometer – Identifying the major business risks for 2023", https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, January 2023.

Security Threats in Cloud-based Services Panel #3

"Cyber risks, such as IT outages, ransomware attacks or data breaches, rank as the most important risk globally (34 % of responses) for the second year in succession – the first time this has occurred."

Image: Image by Gerd Altmann from Pixabay

Statement: AGCS, "Allianz Risk Barometer – Identifying the major business risks for 2023", https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, January 2023.

Contributors

Moderator:

Prof. Dr. Andreas Aßmuth, Ostbayerische Technische Hochschule Amberg-Weiden, Germany

Panelists:

Sr Lect. Dr. Ian Ferguson, Abertay University, UK

Prof. Dr.-Ing. Christoph P. Neumann, Ostbayerische Technische Hochschule Amberg-Weiden, Germany

Lieutenant Colonel Dr. Gerhard Schwarz, Bundeswehr (German Armed Forces), Germany

Dr. Jyrki Penttinen, Syniverse, USA

Top 5 Threats in Cloud Computing:

1. Data Breaches
2. Inadequate Access Controls
3. Insecure APIs and Reliance on 3rd Party Software
4. Malicious Insiders
5. Account Hijacking

Top 5 Threats in Cloud Computing:

1. Data Breaches
2. Inadequate Access Controls
3. Insecure APIs and Reliance on 3rd Party Software
4. Malicious Insiders
5. Account Hijacking

Today, Cloud Computing is an established technology. Most security problems are not cloud-specific, but already known from other systems.

After 40 years of failing to teach users to use strong passwords and a minimum level of awareness, we should think about developing access systems that use AI to recognize the user. This would solve many security problems.

Cloud Computing? Security? It's **still** someone else's computer...

Do you trust their

- Integrity?
- Ability?

In so many layers:

- Hardware
- OS
- Application
- Configuration/operation
- Hypervisor
- Crypto
- Networking

Cloud Computing is **still** fundamentally untrustable.

Prof. Dr.-Ing. Christoph P. Neumann Panelist Position

- Security threats in cloud-based services. . . are a significant cause for social concern in an interconnected world increasingly reliant on cloud technologies.
- Recognizing and mitigating these threats must become as ubiquitous to computer science as unit testing. It begins with the little things, forming the security mindset.

Lieutenant Colonel Dr. Gerhard Schwarz Panelist Position

Security starts with a robust design, why not state-of-the-art, followed by a solid, resilient implementation, and with it, competent operation.

Cloud Computing, applications or microservices, even dynamic content meshes do not contradict good security! Therefore: Business as usual!

Dr. Jyrki Penttinen Panelist Position

New mobile communications era and enhanced protection

- Facilitated by Service Based Architecture (SBA) and Network Functions Virtualization (NFV), cloud environment can be used to efficiently serve the radio and core features – it will be essential in 5G and beyond.
- 3GPP has designed 5G renewing also the integrated security by design – not leaving it as an afterthought. Thus, e.g., the network functions on cloud are authorized and mutually authenticated prior to their protected communications.
- Nevertheless, regardless of the preparation for imaginable attack vectors and foreseen threat models, new technologies and open SW may also result in completely new, still unknown possibilities for fraudsters.

Way forward

- Mobile ecosystem needs to cooperate to efficiently identify and protect against the new threats on time.
- Constant monitoring and information sharing are elemental ways as they benefit the stakeholders and end-users, protecting their assets and IDs.

Open Discussion

- Panelists and audience question whether AI for authentication based on biometrics or behaviour is practical and acceptable to most users
- In terms of trust and authentication, instead of the current binary decision, solutions will need to be more fine-grained in the future
- Security should not be taught separately, but in every computer science course, not in detail, but to keep (future) computer scientists interested and aware of security
- In 5G, the communication world has changed significantly compared to previous versions of mobile networks; now, the mobile networks, the Internet and the Cloud are growing together
- With 5G, mobile operators can give CSPs responsibility for their core network
- Discussion about whether 5G network components are the weakest link in the overall infrastructure and, therefore, must not be sourced from other countries – or is this just an assertion to achieve a better market position for manufacturers of the own country?

The organizers and panelists would like to thank everyone for their interest and comments.